PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-234330
(43)Date of publication of application : 27.08.1999

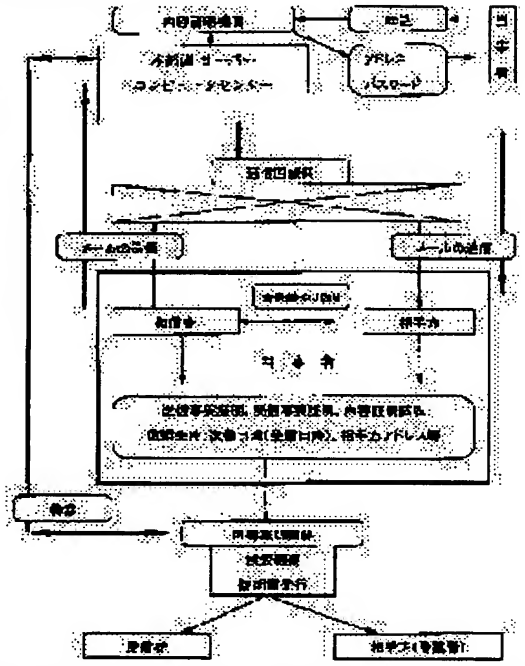
(51)Int.Cl. H04L 12/54
H04L 12/58
G06F 13/00
G09C 1/00
H04L 9/32

(21)Application number : 10-063809
(22)Date of filing : 09.02.1998

(71)Applicant : NAGASHIMA KATSUYOSHI
(72)Inventor : NAGASHIMA KATSUYOSHI

(54) ELECTRONIC MAIL TRANSMISSION CONTENTS CERTIFICATION SYSTEM DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device as a more convenient instrument for growing out of a contents certification means by document transmission utilizirig conventional mail, realizing contents certification on electronic mail suited to the change of times as a new means and contributing to a society by certifying the exchange of the electronic mail between persons concerned by a third person.
SOLUTION: This device is composed of the means for certifying the communication fact of the electronic mail exchanged through a communication medium and the contents to the third person instead of the person concerned when the person concerned needs to certify the communication fact and the contents later by the method of temporarily recording them in a computer center and transmitting them to an opposite party thereafter. Thus, a contract is executed at ease in an electronic mail society. Also, purchase utilizing the electronic mail is accelerated more and products are received in a short time. Further, for a trouble by the electronic mail, the contract contents are correctly managed and certified.



LEGAL STATUS

[Date of request for examination] 23.02.2000
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－234330

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/54		Ｈ０４Ｌ	11/20	１０１Ｂ
	12/58		Ｇ０６Ｆ	13/00	３５１Ｇ
Ｇ０６Ｆ	13/00	３５１	Ｇ０９Ｃ	1/00	６４０Ｄ
Ｇ０９Ｃ	1/00	６４０			６４０Ｚ
			Ｈ０４Ｌ	9/00	６７３Ａ

審査請求　未請求　請求項の数５　書面　（全　６　頁）　最終頁に続く

(21)出願番号　特願平10－63809

(22)出願日　平成10年(1998)２月９日

(71)出願人　596155786
長嶋　克佳
神奈川県相模原市新磯野３丁目４番７号

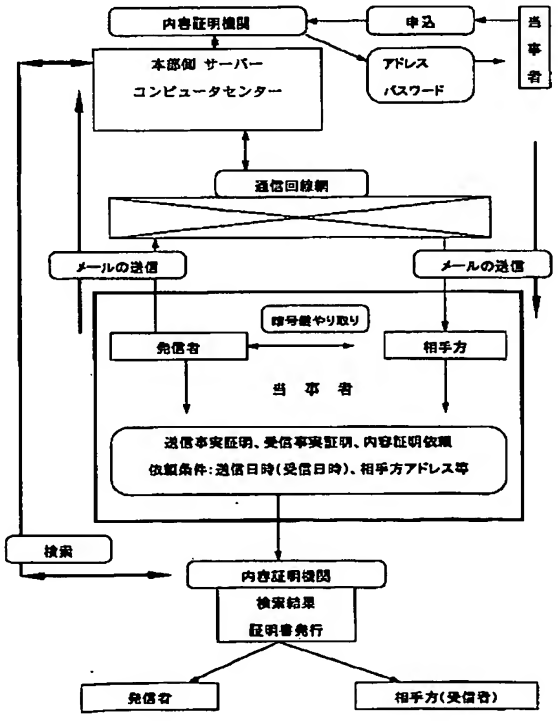
(72)発明者　長嶋　克佳
神奈川県相模原市新磯野３丁目４番７号

(54)【発明の名称】　電子メール送信内容証明システム装置

(57)【要約】　（修正有）

【課題】　当事者間の電子メールのやり取りを第三者が証明する事で、従来の郵便を利用した書面送付による内容証明手段から脱却し、時代の趨勢に即した電子メール上での内容証明を新たな手段として実現し、より便利な社会に貢献する道具として本発明装置を提供する。

【解決手段】　この装置は、通信媒体を介してやり取りされる、電子メールの通信事実及びその内容を一旦コンピュータセンターに記録し、その後相手方に送信する方法で、当事者が後日その通信事実や内容を証明する必要があるとき、当事者に代わって第三者に証明する手段とから構成されている。



1

【特許請求の範囲】

【請求項１】　本発明装置は、通信媒体を介して送信されるあらゆる電子メールに関し直接相手方に送信する方法で無く、送信内容を一旦コンピュータセンターに送信しその送信内容を記録した後、そのセンターから相手方に自動送信する手段と、

後日当事者が送信内容を第三者に証明する必要が生じたとき、コンピュータセンターに記憶された、その送信内容を当事者に代わって第三者に証明する手段を具備したことを特徴とする電子メール送信内容証明システム装置。

【請求項２】　相手方に送信をするときは、送信するメールを事前に暗号鍵を使い内容証明システム独自な暗号化プログラムを起動し、相手方送信アドレスを含み全ての内容を暗号化すると共に、あらかじめコンピュータセンター側から与えられた送信アドレスを使い送信を実行することで、自動的にコンピュータセンターにメールが送信され送信内容が記録される手段を具備したことを特徴とする電子メール送信内容証明システム装置。

【請求項３】　さらにコンピュータセンターから相手方に送信するとき、暗号化されたメールの中にある相手方アドレスのみを覗く暗号鍵で、相手方アドレスを認識し相手方に送信する手段を具備したことを特徴とする電子メール送信内容証明システム装置。

【請求項４】　コンピュータセンターから相手方に送信されたメールの表題に第二の暗号鍵を入力する方法のメッセージを表示し、第二の暗号鍵のみで機密を守り、その鍵を使ってメール全文を開く手段を具備したことを特徴とする電子メール送信内容証明システム装置。

【請求項５】　さらに第一の暗号鍵と第二の暗号鍵を併用する事で機密を２重に管理し、その鍵を使ってメール全文を開く手段を具備したことを特徴とする電子メール送信内容証明システム装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、通信媒体を介して送信されるインターネット上での電子メールに関して、メールが相手方に送信された場合、その事実と内容を第三者に証明するシステム装置を提供する。

【０００２】

【従来の技術】これまで書面等の配達を証明する手段は、郵便局による配達証明、内容証明であった。　しかしながら通信手段の発達した現代社会において従来の手段では、解決出来ない問題が多発している。郵便物は、書面の郵便、宅配、テレックス、ＦＡＸを中心とした時代から、インターネット、ＦＡＸ等を中心とした通信手段を利用した送信方法へ激変している。さらに世界が２４時間で動いている現状、世界が瞬時につながる現状の中で電子メールが確かに相手に到着したか、本人が見たか、後日相手に対しメール上のやり取りを証明し、問題

2

の解決を必要とする時代となっている。　しかしながら未だ実現されていない。

【０００３】

【発明が解決しようとする課題】これらの事から、今後電子メール上での契約の行為が日常茶飯事に行われ、さらに国際間での同様な行為は日に日に増大する事から、当該契約でのトラブル多発は、容易に想像できる。　従って緊急の課題として当事者間の電子メールのやり取りを第三者が証明する事で、従来の郵便を利用した書面送付による内容証明等の手段から脱却し、時代の趨勢に即した電子メール上での内容証明を新たな手段として実現し、より便利な社会に貢献する道具として本発明装置を提供する。さらに一般的な、見積書、契約書、発注書、申込書等もこれを利用する事で、より安全な行為を行う道具となる。　これにより発生が予想される問題点を根本的に解決し、より安心できる契約社会を実現する事を目的とする。

【０００４】

【課題を解決するための手段】本発明は、これらの課題を解決する手段として本発明装置を提供する。　この装置は、通信媒体を介してやり取りされる電子メールの通信事実及びその内容を当事者に代わって第三者に証明する手段を提供する事である。

【０００５】具体的にインターネットと本発明装置の例で述べれば、本発明装置を利用する者は、原則的に本発明装置を提供する側に必要事項を登録する。　その後本発明装置を提供する側から本人識別のアドレスとパスワードが与えられる。　送信者は、送信メールと共にこのアドレスをコンピュータ端末から入力し送信を実行すると、コンピュータセンターに全文が配信される。　コンピュータセンターは、このメールを受信すると発信者のアドレスを認識し、発信者のアドレスと受信順に管理される番号（管理番号）ごとに、記憶装置に所定の方法でその全文を記録する。　この記録された内容は、半永久的に保存される。　このとき受信した全文と共に受信した日時も記録される。　発信者がインターネット未加入者の送信、ＦＡＸから直接送信の場合は、このセンター側にある音声応答装置を介して受信する事もできる、このときはアドレスに代わり電話番号等が利用される。

【０００６】その後、コンピュータセンターの所定のプログラムが起動し、発信の準備に入る。そのため再度記録した全文を呼び出し相手方アドレスに基づき発信する。第一の暗号鍵は、安全を期して別途手段により当事者間でやり取りされる。暗号化されているメールにおいては、このセンター側は、発信者のパスワードを与える事で全文の中にある「相手方アドレスと第二の暗号化要・不要付フラッグ」のみを認識できる。その後、第二の暗号化要・不要付フラッグが「要」のとき所定の表題（相手方に対しメッセージを伝えるための頁）を作成し全文の内容をインターネットの手順に従い相手方に送信

する。第二の暗号化要・不要付フラッグが「不要」の場合は、あたかも発信者から直接配信したかのようにするため、表題をつけない場合もある。表題をつける場合は、通常の暗号鍵の他に第二の暗号鍵を付加できる機能がある。このセンターから相手方に送信したと同時に、記憶装置にある該当全文に、送信したときの日時等履歴に必要な事項を付加し記録する手段がある。正しく送信されないとき、あるいは相手方に読まれないときは、再度自動送信が行われる手段も用意されている。

【０００７】送信者が相手方に送信しようとしたとき、「送信者及び相手方」（当事者）のみが知りうる暗号鍵を用いて、内容証明システム独自の暗号化プログラムが起動し、インターネット上で必要とする情報以外の送信する全文が暗号化される。従って当事者以外、どこにどのような内容の書面が送付されたかわからない様なセキュリティー管理の工夫も用意されている。　コンピューターセンター側は、相手方アドレスのみに限って閲覧できるのみである。　従って従来のインターネットでは、実現出来ないセキュリティー手順が用意されている。

【０００８】さらに暗号化での特徴を述べれば、まずコンピュータセンター側でのメールを覗く権限は、「相手方アドレスと第二の暗号化要・不要付フラッグ」に限る手段となっている。送信する全文は、当事者のみが知りうる暗号鍵で暗号化されている。　相手方のアドレスをコンピュータセンター側が知りうる手段は、例えば送信者のアドレスとパスワードとで覗く事ができる「相手方アドレスと第二の暗号化要・不要付フラッグ」が記憶されたヵ所のみである。「相手方アドレスと第二の暗号化要・不要付フラッグ」を覗く鍵は、発信者とコンピュータセンターのみが本発明装置を利用する前に互いに約束し決定される手段となっている。

【０００９】又、暗号鍵の利用方法は、　第一の暗号鍵と第二の暗号鍵を併用する場合、　第一の暗号鍵のみ、　第二の暗号鍵のみ、　全く暗号鍵を利用しない場合、それぞれ必要に応じて選択できる。第一の暗号鍵は一般的手順のものを利用するが、第二の暗号鍵は、例えば名前、役職、等である。　インターネット上では、全文が暗号化されている事で第三者が知りうる範囲は、「可能性としては当事者のアドレスのみ」であることから、通信回線上で当事者の名前、役職は、第三者が知り得ない鍵となりうる。　さらに「その当事者を知り得る者」が極秘パスワードも知った上で閲覧できる可能性を防止するためには、「その当事者を知り得る者」が閲覧出来ない万全の工夫として、第一の鍵と併用する手段もある。

従ってセキュリティーの度合いから、前記方法の組み合わせを選択し暗号鍵を用いる柔軟な手段が用意されている。

【００１０】さらに具体的な例は、互いが暗号鍵を知らない場合あるいは相手に暗号鍵を知らせる事が出来ないときで、かつ第三者に知られたくないメールを発信するときの手段である。　このときの一例を挙げれば、第二の鍵として相手方の名前を利用する。　この鍵は、少なくともインターネット手順において、当事者を知りうる者以外が通信回線上で暗号を解読する事ができない。第二の鍵を相手方に知らせる方法であるが、例えば表題に暗号鍵が名前のときは名前を入力する指示を明記する事で暗号鍵を渡す事ができる手段がある。　その手段は、相手方に対し都度知らせる必要がないのでセキュリティー上のメリットがある、例えばあなたの名前を入力してくださいとメッセージを伝える事で済む。

【００１１】当事者が、送信した事実証明、内容証明等を必要とした場合は、当事者に代わって本発明装置を提供する者が証明する。　その手段は、依頼を受けた当事者からアドレス、送信日時とあらかじめ本発明装置を提供する側から知らされた管理番号を基に証明依頼をする事で実行される。　本発明装置を提供する側は、メールが暗号化されている場合解読が必要となる。よってこの時、依頼を受けた当事者から使用した暗号鍵が知らされ、初めて全文の内容を知る事が出来る手段となっている。

【００１２】本発明装置を提供する側から証明する内容は、発信者の情報（名前、住所、電話番号等）、センターの受信日時、相手方アドレス、センターから相手方への送信日時、送信全文内容等を第三者としてコンピュータ記録事実に基づき証明する手段である。　さらに本発明装置の他に法的な問題を抱える事から証明する機関を設け、しかるべき弁護士が対応する手段も用意されている。

【００１３】

【実施例】以下、本発明装置の一実施例を図面を用いて詳細に説明する。図１は、本発明による電子メール送信内容証明システム装置のコンピュータセンター側一実施例の構成を示す図である。　本装置は、コンピュータ１とそれに接続される、ディスプレイ（画面）２、キーボード３、フロピーディスク４、ハードディスク５、プリンター６、その他必要な外部装置７、及びプログラムとから構成されている。　コンピュータ１には、ネットワークを構築するための電話回線ケーブル８が接続されている。　もちろん通信装置９を内臓している。　さらに本発明装置を利用する側には、インターネット関連ソフトウェアー、通信装置の他に必要の都度暗号化のための所定のプログラムを内蔵する。

【００１４】ネットワークで結ばれている各端末から入力された各メールは、通信回線を経由してコンピュータ１に送信される。　送信されたメールは、発信者アドレスとパスワードをコンピュータ１が認識し、コンピュータ１に記憶されている「アドレス及びパスワード」と一致しているとき、所定のプログラムが起動しそのアドレスが持つ記憶領域のハードディスク５に着信順に管理されている番号を付加し記憶される。　アドレスでなく、

それに代わる電話番号のときは、別途用意されたプログラムが音声応答システムを利用し、同様な処理をする事となる。

【００１５】さらにコンピュータセンターの所定のプログラムが起動し相手方に送信する準備が開始される。この時プログラムは、発信者から得られた第二の暗号化要・不要フラッグと相手方アドレスのみを認識し全文を送信する。　その後コンピュータセンターからインターネット手順に基づく情報（相手先に正しく送信されたか、読んだか等）の監視が行われ、その結果がコンピュータセンター側に記憶される。正しく送信されないとき、あるいは読まれないときは、再度自動送信が行われる。それでも尚、読まれない場合は、人間介在の直接電話での緊急依頼等の手段がある。相手方に送信した後の情報（送信した日時、読まれたか否か等）は、発信者に所定の方法で返信される。

【００１６】その後当事者が、送信内容・受信内容の証明依頼を希望したときは、ハードディスク５に記憶されている情報から当事者のアドレスと（発信日時あるいは受信日時）と管理番号とを条件に検索し、記録されている情報を書面等に復元し認証を行い、依頼者に渡す。さらに必要に応じ第三者への証明を行う。

【００１７】

【発明の効果】本発明の電子メール送信内容証明システム装置によれば、

電子メール社会で契約を安心して遂行出来る。

電子メール利用の購買が益々促進され、短時間に商品を受け取る事ができる。

電子メールでのトラブルに対し、その契約内容を正しく管理し、証明できる。

電子メールでの契約が、個人的レベルにおいても増大し、世界的エリアーで加速される。　従って、今後電子メール利用により発生するであろう、あらゆる諸問題を本発明装置が画期的方法で解決し、情報化を促進出来る。

【図面の簡単な説明】

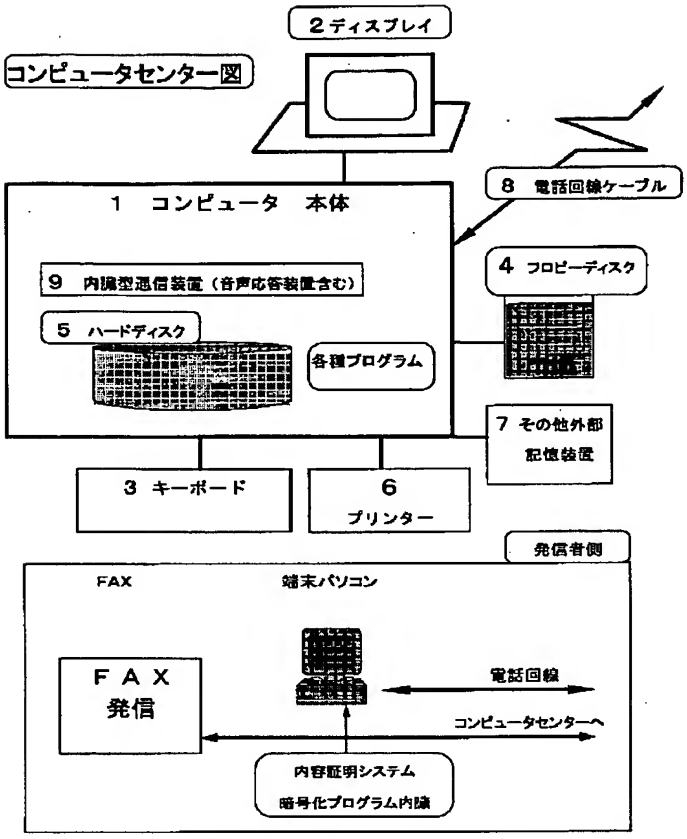
【図１】本発明による電子メール送信内容証明システム装置のコンピュータセンター側及び発信者側の一実施例の構成を示すブロック図である。

【図２】本発明装置を利用したネットワーク図である。

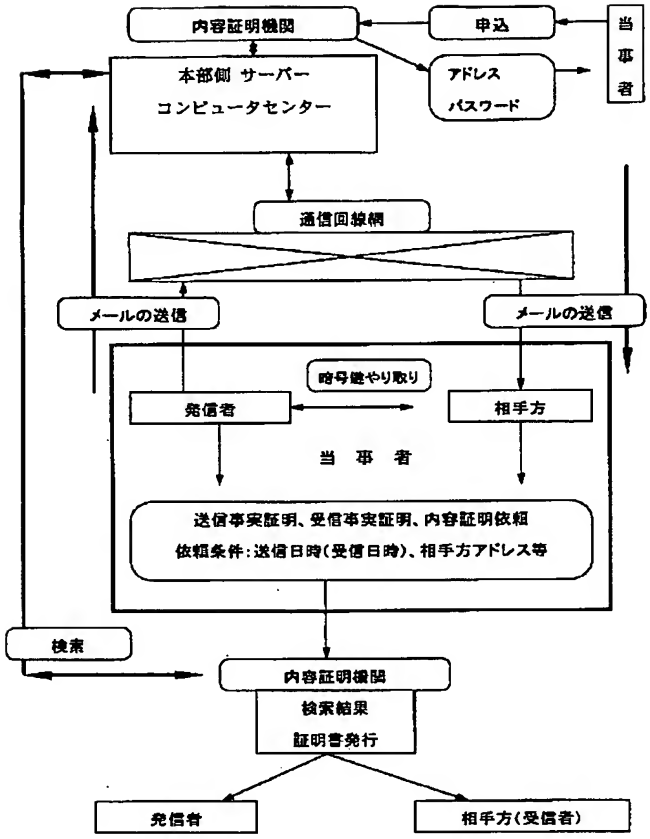
【符号の説明】

１．コンピュータ
２．ディスプレイ
３．キーボード
４．フロピーディスク
５．ハードディスク
６．プリンター
７．その他外部記憶装置
８．電話回線ケーブル
９．内蔵型通信装置

【図１】


コンピュータセンター図
2 ディスプレイ
8 電話回線ケーブル
1 コンピュータ 本体
9 内臓型通信装置（音声応答装置含む）
5 ハードディスク
各種プログラム
4 フロピーディスク
7 その他外部記憶装置
3 キーボード
6 プリンター
発信者側
FAX
端末パソコン
F A X 発信
電話回線
コンピュータセンターへ
内容証明システム
暗号化プログラム内臓

【図２】



フロントページの続き

(51) Int. Cl. [6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ